REMARKS

Applicant appreciates the Examiner's attention to this application. Reconsideration of the application in view of the enclosed amendments and remarks is respectfully requested.

ARGUMENT

At the time of the second Office Action, claims 1-24 and 30-34 were pending. The second Office Action rejects all of those claims based on 35 U.S.C. § 103(a). Applicant respectfully traverses all of those rejections. Among other errors, the rejections in the second Office Action are based on an unreasonably broad interpretation of claim terms such as "network monitoring digital contract." For instance, despite Applicant's explanation regarding the term "network monitoring digital contract" in response to the first Office Action, the second Office Action asserts that an "email message" is the same thing as a "network monitoring digital contract." No reasonable person of ordinary skill in the art would consider those two terms to have the same meaning.

However, in an attempt to avoid the substantial delays and expenses frequently associated with the appeal process and any subsequent prosecution required, this response rewrites the claims to clarify terms such "network monitoring digital contract." In particular, this response cancels claims 1-24 and 30-34 and enters new claims 35-53. Claims 35, 43, 47, and 49-53 are the pending independent claims. Applicant respectfully traverses all of the rejections in the second Office Action, to the extent that they might be applied to the pending claims.

Claims 1-3, 12-16, 23-24, and 30-32

The Office Action rejects claims 1-3, 12-16, 23-24, and 30-32 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent no. 6,442,686 to Mark J. McArdle et al. (hereinafter "McArdle"), in view of U.S. patent no. 6,253,322 to Seiichi Susaki et al. (hereinafter "Susaki").

As was explained in response to the first Office Action, McArdle pertains to a method for enforcing security policies through use of a "policy management agent." Specifically, the policy management agent is interposed between clients and a standard mail server, and the policy management agent intercepts email from the clients before the email reaches the mail server, to prevent the mail server from sending the email if the email violates email security policies. (Abstract.)

In particular, McArdle indicates that the policy management agent may be used to enforce email policies such as the following: a policy that all email must not be encrypted, a policy that all email must be encrypted, and a policy that all email must be encrypted with a key from a predetermined pool of keys (Abstract). Accordingly, McArdle discusses determining whether email is encrypted and other encryption characteristics (col. 12, line 43 – col. 13, line 14). However, the policy management agent in McArdle does not actually decrypt any of the email messages. Accordingly, McArdle does not disclose or suggest that an entity should monitoring decrypted versions of messages that are not addressed to the entity. Determining whether a message is encrypted and actually decrypting the message are two very different operations. McArdle says nothing about allowing a network monitoring element to monitor unencrypted versions of encrypted messages that are not addressed to the network monitoring element.

As was also explained in response to the first Office Action, Susaki pertains to a method for archiving electronic contracts. The contracts are archived or escrowed by a system referred to as a "service providing unit." Specifically, when two (or more) parties want to enter into a contract that is memorialized in electronic or digital form, those parties (which Susaki refers to as "service receiving units") electronically sign the electronic contract and then send the signed copies to the escrow service (i.e., to the service providing unit). The service providing unit then consolidates the contracts into a single document, signs that document, and archives that document. The service providing unit thus serves as an escrow agent for electronic contracts.

In particular, Susaki explains that a party may encrypt a contract before sending the contract to a recipient, and that the intended recipient may then decrypt

the contract (col. 12, lines 12-17). However, Susaki say nothing about allowing a contract to be decrypted by any entity other than an intended recipient. Accordingly, Susaki says nothing about allowing a network monitoring element to monitor unencrypted versions of encrypted messages that are not addressed to the network monitoring element.

By contrast, the present application pertains to methods and systems that support the monitoring of an unencrypted version of an encrypted message, with the monitoring to be performed by an entity other than the intended recipient of the message. As pointed out in response to the first Office Action, pages 7-9 of the Detailed Description explain that a network monitoring digital contract memorializes an agreement between a policy administrator and a network monitoring element to authorize the network monitoring element to monitor communications from network elements.

Furthermore, claim 35 explicitly recites a method involving a "policy administrator" that sends a "network use digital contract" to a "network element," wherein the network use digital contract comprises a term "to allow encrypted communications from the network element to be decrypted by an entity other than addressees of the encrypted communications." In addition, claim 35 recites sending a "network monitoring digital contract" from the policy administrator to a network monitoring element, wherein the network monitoring digital contract comprises a term to allow the network monitoring element to monitor communications from the network element "even if the encrypted communications are not addressed to the network monitoring element." Claim 35 also recites sending decrypting information from the policy administrator to a "network monitoring element" in accordance with a "network monitoring digital contract," with the decrypting information "to allow the network monitoring element to monitor a decrypted version of an encrypted communication from the network element."

As indicated above, McArdle and Susaki do not disclose or suggest allowing a network monitoring element to monitor unencrypted versions of encrypted messages that are not addressed to the network monitoring element.

Consequently, even if McArdle and Susaki were to be combined, the combination would not establish a *prima facie* case of obviousness for claim 35.

Similarly, claim 43 involves a network monitoring element that receives a network monitoring digital contract, wherein the network monitoring digital contract comprises a term to allow the network monitoring element to monitor communications from the network element "even if the encrypted communications are not addressed to the network monitoring element." In addition, the network monitoring element receives decrypting information from the policy administrator, with the decrypting information "to allow the network monitoring element to monitor decrypted versions" of encrypted communications from the network element. As indicated above, McArdle and Susaki do not disclose or suggest allowing a network monitoring element to monitor unencrypted versions of encrypted messages that are not addressed to the network monitoring element. Consequently, even if McArdle and Susaki were to be combined, the combination would not establish a *prima facie* case of obviousness for claim 43.

Similarly, claim 47 involves a network element that receives a network use digital contract from a policy administrator, wherein the network use digital contract comprises a term to indicate that the network element has agreed "to allow encrypted communications from the network element to be decrypted by an entity other than addressees of the encrypted communications." As indicated above, McArdle and Susaki do not disclose or suggest allowing messages to be decrypted and monitored by any entity other than an intended recipient. Consequently, even if McArdle and Susaki were to be combined, the combination would not establish a *prima facie* case of obviousness for claim 47.

Claims 49-53 are patentable over McArdle and Susaki for the same or similar reasons as those applicable to claims 35, 43, and/or 47. In addition, the dependent claims implicitly include the features of their respective parent claims. Consequently, even if McArdle and Susaki were to be combined, the combination would not establish a *prima facie* case of obviousness for any of the pending claims.

Moreover, as also was explained in response to the first Office Action, neither McArdle nor Susaki provide any motivation for combining an escrow agent for electronic contracts with a policy management agent for email.

It is well settled that, for an obviousness rejection to be valid, any motivation to combine must come from the prior art. For instance, as explained in section 2143.01 of the Manual of Patent Examining Procedure (MPEP), "[t]he mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination" (citing to *In re Mills*, 916 F2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990)). Nothing in either McArdle or Susaki teaches that it would be desirable to combine an escrow agent for electronic contracts with a policy management agent for email. Similarly, nothing in either McArdle or Susaki teaches that it would be desirable to modify a policy management agent for email to include features from an escrow agent for electronic contracts.

The second Office Action asserts that "it would have been obvious ... to modify the teachings of McArdle with the teachings of Susaki to include communicating of decrypting information and authenticating the communicated information with the motivation to provide for reliable electronic commerce using cryptographic technologies." It is difficult to determine what that assertion is supposed to mean, but it seems to be saying that Susaki recognizes the desirability of reliable electronic commerce, and that recognition in Susaki would motivate one of ordinary skill in the art to modify McArdle in some manner to provide for more reliable electronic commerce. However, McArdle is not concerned with reliable electronic commerce. To the contrary, McArdle drops email messages if they do not comply with security policies, which may interfere with electronic commerce more than promoting it. Instead, McArdle is concerned with enforcing email security policies.

In actuality, the alleged motivation to combine seems to be based simply on a possible benefit to be derived from the combination, in light of the present application, and not based on any explicit teaching or suggestion in McArdle or Susaki regarding the possibility of combining a policy management agent for email

with an escrow agent for electronic contracts. In particular, the alleged the motivation to combine appears to be based entirely on hindsight, in view of the present application. It is well established, however, that hindsight is not a proper basis for the motivation to combine.

For these and other reasons, all rejections based on a combination of McArdle and Susaki are improper.

Claims 4-11, 17-19, and 33-34

The second Office Action rejects claims 4-11, 17-19, and 33-34 under 35 U.S.C. § 103(a) as being unpatentable over McArdle and Susaki, in view of U.S. patent no. 6,324,645 to Richard F. Andrews et al. (hereinafter "Andrews").

As indicated in the response to the first Office Action, Andrews pertains to a method for managing a "public key infrastructure," such as the infrastructure used by a certification authority (CA) for managing and authenticating digital certificates (col. 6, lines 35-43). In particular, Andrews pertains to a method for controlling access to the infrastructure, based on digital certificates associated with users of the infrastructure. For instance, Andrews discloses a process for creating a digital certificate for a user, in which an "access label" is included in the digital certificate to identify access rights for the user (col. 12, lines 24-44).

McArdle, Susaki, and Andrews do not provide a motivation for combining (a) an escrow agent for electronic contracts, (b) a policy management agent for email, and (c) a method for controlling access to a public-key management infrastructure. The second Office Action asserts that "it would have been obvious ... to modify the teachings of Andrews to include computer-implemented techniques based on digital certificates with the motivation to efficiently allow multiple users to share a public key management infrastructure, while simultaneously managing risk associated with such sharing." It is difficult to determine what that assertion is supposed to mean, but it seems to be saying that Andrews recognizes the desirability of efficiently sharing a public key management infrastructure, and that recognition in Andrews would motivate one of ordinary skill in the art to modify Andrews, in some

unspecified manner, to "include computer-implemented techniques based on digital certificates."

A vague assertion that Andrews provides motivation to modify Andrews to "include computer-implemented techniques based on digital certificates" is nowhere near sufficient basis to establish motivation to combine (a) an escrow agent for electronic contracts, (b) a policy management agent for email, and (c) a method for controlling access to a public-key management infrastructure. What would be needed for a valid obviousness rejection is a more specific explanation of which statements (if any) in McArdle, Susaki, and/or Andrews specifically recognize the desirability of combining (a) an escrow agent for electronic contracts, (b) a policy management agent for email, and (c) a method for controlling access to a public-key management infrastructure. However, the second Office Action provides no such explanation. This omission should not be surprising, however, because McArdle, Susaki, and Andrews do not contain the kinds of statements that would be required to provide a motivation to combine McArdle, Susaki, and Andrews in the manner alleged in the second Office Action.

Consequently, the motivation to combine that is alleged in the second Office Action appears to be based entirely on hindsight, in view of the present application. It is well established, however, that hindsight is not a proper basis for the motivation to combine. For these and other reasons, all rejections based on a combination of McArdle, Susaki, and Andrews are improper.

Furthermore, even if McArdle, Susaki, and Andrews were to be combined, the combination would merely create a data processing system that (a) allows service receiving units to escrow digital contracts, (b) monitors email messages to enforce security restrictions, and also (c) creates digital certificates that include includes access labels which identify access rights within a public-key management infrastructure. The combination would not disclose or suggest allowing a network monitoring element to monitor unencrypted versions of encrypted messages that are not addressed to the network monitoring element.

In particular, the combination would not disclose or suggest a "policy administrator" that sends a "network use digital contract" to a "network element,"

wherein the network use digital contract comprises a term "to allow encrypted communications from the network element to be decrypted by an entity other than addressees of the encrypted communications." The combination also would not disclose or suggest sending decrypting information from the policy administrator to a "network monitoring element" in accordance with a "network monitoring digital contract," with the decrypting information "to allow the network monitoring element to monitor a decrypted version of an encrypted communication from the network element," even if the communication is not addressed to the network monitoring element. (Claim 35.)

The combination also would not disclose or suggest a network monitoring element that receives a network monitoring digital contract from a policy administrator, and that receives decrypting information from the policy administrator, with the decrypting information "to allow the network monitoring element to monitor decrypted versions" of encrypted communications from a network element, even if the communications are not addressed to the network monitoring element. (Claim 43.)

The combination also would not disclose or suggest a network element that receives a network use digital contract from a policy administrator, wherein the network use digital contract comprises a term to indicate that the network element has agreed "to allow encrypted communications from the network element to be decrypted by an entity other than addressees of the encrypted communications." (Claim 47.)

Claims 49-53 are patentable over McArdle, Susaki, and Andrews for the same or similar reasons as those applicable to claims 35, 43, and/or 47. In addition, the dependent claims implicitly include the features of their respective parent claims. Consequently, even if McArdle, Susaki, and Andrews were to be combined, the combination would not establish a *prima facie* case of obviousness for any of the pending claims.

Claims 20-21

The second Office Action rejects claims 20-21 under 35 U.S.C. § 103(a) as being unpatentable over McArdle in view of Andrews.

The second Office Action admits that "McArdle does not expressly disclose a network monitoring element establishing a network monitoring digital contract with a policy administrator." However, the second Office Action asserts that Andrews discloses a network monitoring element establishing a network monitoring digital contract with a policy administrator. That assertion is incorrect.

Claim 35 involves sending a "network use digital contract" from a policy administrator to a network element, wherein the network use digital contract comprises a term "to allow encrypted communications from the network element to be decrypted by an entity other than addressees of the encrypted communications." In addition, claim 35 involves sending a "network monitoring digital contract" from the policy administrator to a network monitoring element, wherein the network monitoring digital contract comprises a term "to allow the network monitoring element to monitor communications from the network element, even if the encrypted communications are not addressed to the network monitoring element." Claim 35 also involves sending decrypting information from the policy administrator to the network monitoring element in accordance with the network monitoring digital contract and the network use digital contract, the decrypting information "to allow the network monitoring element to monitor a decrypted version of an encrypted communication from the network element." Thus, according to claim 35, the network monitoring element is allowed to monitor decrypted versions of encrypted communications that are not addressed to the network monitoring element.

As indicated above, McArdle does not disclose or suggest allowing decrypted versions of messages to monitored by any entity other than intended recipients. Also, Andrews does not disclose or suggest allowing messages to be decrypted and monitored by any entity other than intended recipients.

Consequently, even if McArdle and Andrews were to be combined, the combination would not establish a *prima facie* case of obviousness for claim 35. For the same or similar reasons, a combination McArdle and Andrews would not

establish a *prima facie* case of obviousness for any of the other independent claims. In addition, the dependent claims implicitly include the features of their respective parent claims. Consequently, even if McArdle and Andrews were to be combined, the combination would not establish a *prima facie* case of obviousness for any of the pending claims.

Additional Recited Features

Moreover, the claims recite additional features that are not disclosed or suggested by the cited art. For instance, claim 42 pertains to an embodiment in which the network use digital contract comprises "data to indicate that the network element has agreed to allow encrypted communications from the network element to a second network element to be decrypted by an entity other than the second network element." Also, claim 37 pertains to an embodiment in which the policy administrator allows the network monitoring element to monitor encrypted communications from a network element by "sending a decryption key from the policy administrator to the network monitoring element, the decryption key to allow the network monitoring element to decrypt the encrypted communication." Claim 38 pertains to an embodiment in which the policy administrator allows the network monitoring element to monitor encrypted communications from a network element by sending a "decrypted communication" from the policy administrator to the network monitoring element. The prior art does not disclose or suggest any of these features.

For reasons including those set forth above, the second Office Action fails to make out a *prima facie* case of obviousness for any of the pending claims.

CONCLUSION

Claims 35-53 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927. Prompt issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: 2/7/05

/ Michael Barre /

Michael R. Barré
Registration No. 44,023
Patent Attorney
Intel Americas, Inc.
(512) 732-3927

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026